Here are several VERY interesting developments:
the LAO Report on HIPAA,
DHHS reopening the HIPAA privacy act comment period, and
Clarifications (opinions) on entity types.

Hope you enjoy!!!
Ken

There is a new Legislative Analyst Office report related to HIPAA that can be accessed at:
www.lao.ca.gov/analysis_2001/health_ss/hss_2_CC_HIPAA.htm

Contents:

********** [hipaalive] Privacy: Comment period to be opened **********
>>> luba@san.rr.com 02/23/01 03:49PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

FYI...from AHA News

Secretary of Health and Human Services Tommy Thompson said today the department is reopening the HIPAA privacy act regulations for a new, 30-day comment period. An HHS spokesman said he did not know when that period will begin; he said details will be published in the Federal Register next week. In his statement, Thompson said, "Our goal is to achieve privacy protection that works. I believe we should be open to the concerns of all those who care strongly about health care and privacy. And after we hear those concerns, our commitment must be to put strong and effective patient privacy protections into effect as quickly as possible." Thompson also confirmed that the effective date of the Health Insurance Portability and Accountability Act privacy regulations has been extended to April 14 because of a bureaucratic snafu in the last days of the Clinton Administration. It was not immediately known whether that extension and the 30-day comment period would overlap.

********** Re: [hipaalive] GENERAL: State Specific Requirements **********
>>> Rob.Lathrop@mhn.com 02/23/01 01:54PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

I was just in a meeting where I was informed that New Jersey is requiring the data set portion of HIPAA is due 01/01/2002. My company has an office there and exchanges data. Do I need to know every state where we conduct business and find out their requirements? Or do I follow the requirements of the state where I am located?

********** [hipaalive] Re: PRIVACY: Health plans obtaining consent **********
>>> ApgarC@providence.org 02/23/01 09:13AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Two qualifiers:
1. This only covers providers who elect to directly or indirectly (i.e., through a billing service) send & receive data electronically. Providers who elect not to communicate electronically are not covered and are not required to obtain consent.
2. State statute and accreditation requirements may require payers and others to obtain consent. We are required by Oregon statute and NCQA to obtain consent. While this requirement is not related to HIPAA compliance, I think it is important to remember our overall regulatory environment may well require us to do as much as or more than HIPAA requires ("state law more stringent than...").

Chris Apgar,
Data Security & HIPAA Compliance Officer

********** [hipaalive] Re: PRIVACY: Health plans obtaining consent **********
>>> wmacbain@epix.net 02/23/01 09:06AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Only a provider of health care services is required to obtain a HIPAA consent.

If you are functioning as a health plan, as defined by HIPAA, you don't need the consent to use or disclose PHI (protected health information) for the HIPAA triad: "treatment, payment, or health care operations." You will sometimes need an authorization for certain uses and disclosures that don't fit within the HIPAA triad. The privacy regulations go on for miles regarding when authorizations are and are not required. (Good bed time reading.)

If you are neither a provider nor a health plan, then you are handling PHI as a business associate of a covered entity, and you are not regulated by HIPAA. Each covered entity with which you contract is required to incorporate a number of provisions in their contract with you, binding you contractually to treat the PHI you receive with the same degree of care as HIPAA imposes on the covered entity.

Bill MacBain
MacBain & MacBain, LLC

********** [hipaalive] RE: GENERAL: Consents and Authorizations **********
>>> wmacbain@epix.net 02/23/01 08:55AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Regarding use of a current "Policy Regarding Privacy and Patient's Rights".

HIPAA establishes very specific requirements for the content of a "consent," "authorization," and "notice of privacy practices." You will need to review your current record release and patients' rights forms and policies against the HIPAA regulations and make modifications to comply. Expect significant modifications.

There is no requirement to sign the notice of privacy practices, but it must be referenced in the consent form, which the patient does sign.

I suggest you review the regulations carefully and make some check lists. You have two years to comply, so you don't need to make changes immediately.

Bill MacBain
MacBain & MacBain, LLC

*** This is HIPAAlive! From Phoenix Health Systems ***
RE: [hipaalive] Re: PRIVACY: Health plans obtaining consentHIPAA lists a

number of elements that must be in the business associate contract, the intent of which is to extend the protections of HIPAA to PHI disclosed to business associates. Congress didn't provide the authority to regulate the business associate directly, so the regs require the covered entity to regulate its business associate by contract.

HIPAA also requires the covered entities to enforce their contracts when they become aware of any material breach of the privacy requirements of the contract. (This includes termination, or notice to the Secretary of HHS if termination is impracticable, when the breach cannot be cured.)

Your FDA question is interesting. Depending on the reason the information is being disclosed to the FDA, this may come under the public health disclosure rules of section 164.512(b). If so, a covered entity is permitted (but not required) by HIPAA to make the disclosure of PHI without an authorization or a business associate contract.

Bill MacBain
MacBain & MacBain, LLC

********** [hipaalive] RE: "In-house" Referrals ******************
>>> tom.hanks@beaconpartners.com 02/22/01 10:50PM >>>

1) Referrals are part of treatment, payment and health care operations - covered by consent and not authorization required.
2) No authorization is required for sharing information with other providers for the purpose of treatment - again covered by consent
3) Disclosure of Psych notes requires authorization.

ALSO:

1) Business Associate Contract (BAC) has the effect of imposing the same restrictions on a covered entity's business associates as the covered entity would have under HIPAA - except the only sanctions or penalties for the business associate are those enforced by the covered entity through the BAC.
2) HIPAA covers PHI in a covered entity without regard to the source of the PHI (e.g. received from a non-covered entity), how it is created, or the purpose of its creation.

Thanks,

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.

********** [hipaalive] RE: GLB State of Domicile ************
>>> Kenneth.Fody@ibx.com 02/22/01 08:34PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***
I'm not an expert on GLB, but from my observation, I believe this means that states may take authority over enforcement of GLB privacy requirements against insurance carriers. Many states are adopting the NAIC Model Privacy Act/Regulation to give them the necessary authority to enforce GLB. The states must act by July 1, 2001 if they want that responsibility.

One way this does impact HIPAA -- the NAIC Model includes Health information privacy as well as GLB privacy. So carriers could find themselves, IN JULY OF 2001, subject to health information privacy requirements comparable to HIPAA's (HIPAA's privacy regulation is based on the NAIC Model adopted a few years ago).

Ken Fody

********** [hipaalive] RE: Coordination of Benefits (COB) **********
>>> Kenneth.Fody@ibx.com 02/22/01 08:34PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

It may be premature to answer that question. I think Health Plans need to get a better understanding of how the transaction can be used in that fashion, what other health plans are doing (e.g. we won't do it, if they don't ;-), and whether it increases effectiveness/efficiency.

An age old problem with COB is still going to be figuring out when to use the transaction (e.g. when does someone have other coverage).

Ken Fody

********** [hipaalive] RE: PRIVACY: Hybrid Entity **********
>>> tom.hanks@beaconpartners.com 02/22/01 10:50PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Under the hybrid entity concept, the entire entity is not covered under the rule unless what the health component does represents most of the activity of the entity. Otherwise only the health care component is covered and required to comply to HIPAA.

I think it would be rare that the health care activities of a county or state would represent most of the activity of the county or state. There I believe that the entire county or state government would not ordinarily be considered a covered entity - just the health care component.

Tom Hanks
Practice Director, Enterprise Security & HIPAA Compliance
Beacon Partners, Inc.

********** [hipaalive] RE: PRIVACY: Hybrid Entity **********
*** This is HIPAAlive! From Phoenix Health Systems ***

Regarding whether a county government is a hybrid entity when it provides health care.

In HIPAA-speak, "hybrid entity" is a definition, not an option. That is, you are what you are.

The provision of health care services is a covered function under HIPAA. If the component that provides the services is not itself a separate entity, then the entity to which it belongs is a HIPAA hybrid entity. HIPAA's rules apply to the component that does the covered function. The import of being a hybrid entity is that HIPAA requires you to build a high wall and deep moat between the covered functions and the rest of the entity. For instance, you will need policies and procedures, and sanctions, to assure that county government employees who are not involved in providing health care do not have any more access to your health care component's PHI than they would have to the PHI in a private doctor's office.

Bill MacBain
MacBain & MacBain, LLC

********** [hipaalive] "In-house" Referrals **********
>>> kborten@mediaone.net 02/22/01 12:54PM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

Sounds as though you're on the right track. But to get the terminology HIPAA-correct, use of protectected health info for treatment is covered by your

"consent" form, not an authorization form which is different. Under HIPAA it becomes important to keep the terms and their uses straight. Since you're all part of a single entity, you may use a single "joint" consent form. And yes, it should refer to your Notice of Privacy Practices. Be sure to read the rule for the specific content and uses of these two forms and the notice. (I can give you the specific pages if you email me.)

As to whether you should share the data across your entities, even though HIPAA gives carte blanche for treatment purposes, you should still follow the information security principle and Privacy Rule requirement for limiting access to the minimum necessary data. That limitation should never hinder patient care, of course.

Finally, be sure to follow other state and federal laws which could be more stringent than HIPAA, especially if you're handling behavioral, psych, addiction health information.

Kate Borten, CISSP
The Marblehead Group

********** [hipaalive] TCS-plan sponsor on 834 **********
>>> Karen.White@medstat.com 02/22/01 10:28AM >>>
*** This is HIPAAlive! From Phoenix Health Systems ***

The following is from the comment section of the transaction standard published in the Federal Register:
"For example, the enrollment and disenrollment in a health plan transaction is most commonly sent by employers or unions, which are not covered entities, to health plans, which are covered entities. The employer may choose to send the transaction electronically in either standard or non-standard format. The health plan, however, must conduct the transaction as a standard transaction when conducting the transaction electronically with another covered entity, with another part of itself, or when requested to do so by any other entity."

Karen H. White
The MEDSTAT Group

********** [hipaalive] GENERAL: Compliance Timeline **********
>>> CJensen@dhha.org 02/22/01 06:49AM >>>
*** This is HIPAAlive! ***

All the rules will have a consistent timeline structure for compliance.

* Final rule published in the Federal Register
* 60 days after publishing the rule becomes effective (assuming no congressional intervention)
* Compliance is required 2 years after the effective date (3 years for small health plans)

The Transaction and Code Sets rule was published 8/16/00, effective 10/16/00, compliance required 10/16/02.
The privacy rules, due to some inattention to paperwork, are now effective 4/14/01, compliance required 4/14/03 (again assuming no intervention)
The Security final rules have not been published, but when they are - the 26 month timeline will apply.
A exception to this timeline is the yet to be proposed Enforcement rule, which will not have a compliance component.

Further information is available at the HHS website.

> -----Original Message-----
> From: James McVey [SMTP:jmcvey@xactimed.com]
> Sent: Thursday, February 22, 2001 6:47 AM
> To: HIPAAlive Discussion List
> Subject: [hipaalive] RE: GENERAL: Covered Entities
>
> *** This is HIPAAlive! ***
>
> Tom,
> I would appreciate it if somebody could clarify for me:
> When is the compliance date for Transaction, Code sets, privacy,
> and security regulations